PROJETO DE LEI Nº , DE DE DE .

Dispõe sobre a proteção de dados pessoais, a privacidade e dá outras providências.

O CONGRESSO NACIONAL decreta:

TÍTULO I

DA TUTELA DOS DADOS PESSOAIS

CAPÍTULO I

DISPOSIÇÕES GERAIS

Art. 1º Esta lei tem por objetivo garantir e proteger, no âmbito do tratamento de dados pessoais, a dignidade e os direitos fundamentais da pessoa, particularmente em relação à sua liberdade, igualdade e privacidade pessoal e familiar, nos termos do art. 5º, incisos X e XII da Constituição Federal.

Art. 2º Toda pessoa tem direito à proteção de seus dados pessoais.

Art. 3º A presente lei aplica-se aos tratamentos de dados pessoais realizados no território nacional por pessoa física ou jurídica de direito público ou privado, ainda que o banco de dados seja localizado no exterior.

§ 1º A presente lei não se aplica:

I – ao tratamento de dados pessoais realizado por pessoa física para fins exclusivamente pessoais e domésticos, desde que os dados tratados não sejam destinados à comunicação;

II – aos bancos de dados utilizados para o exercício da atividade jornalística e exclusivamente para tal fim.

§ 2º Os bancos de dados instituídos e mantidos para fins exclusivos de segurança pública, defesa, segurança do Estado e suas atividades de investigação e repressão de delitos serão regidos por legislação específica.

Art. 4º Para os fins da presente lei, entende-se como:

I - dado pessoal: qualquer informação relativa a uma pessoa identificada ou identificável, direta ou indiretamente, incluindo todo endereço ou número de identificação de um terminal utilizado para conexão a uma rede de computadores;

II - tratamento: toda operação ou conjunto de operações, realizadas com ou sem o auxílio de meios automatizados, que permita a coleta, armazenamento, ordenamento, conservação, modificação, comparação, avaliação, organização, seleção, extração, utilização, bloqueio e cancelamento de dados pessoais, bem como o seu fornecimento a terceiros por meio de transferência, comunicação ou interconexão;

III - banco de dados: todo conjunto estruturado de dados pessoais, localizado em um ou vários locais, em meio eletrônico ou não;

IV - dados sensíveis: dados pessoais cujo tratamento possa ensejar discriminação do titular, tais como aqueles que revelem a origem racial ou étnica, as convicções religiosas, filosóficas ou morais, as opiniões políticas, a filiação sindical, partidária ou a organizações de caráter religioso, filosófico ou político, os referentes à saúde e à vida sexual, bem como os dados genéticos e biométricos;

V - titular: pessoa física a quem se referem os dados pessoais que são objeto de tratamento nos termos desta lei;

VI - responsável: a pessoa física ou jurídica, de direito público ou privado, a quem competem as decisões referentes às finalidades e modalidades de tratamento de dados pessoais;

VII - subcontratado: a pessoa jurídica contratada pelo responsável pelo banco de dados como encarregado do tratamento de dados pessoais;

VIII - comunicação: ato de revelar dados pessoais a um ou mais sujeitos determinados diversos do seu titular, sob qualquer forma;

IX - difusão: ato de revelar dados pessoais a um ou mais sujeitos indeterminados diversos do seu titular, sob qualquer forma;

X - interconexão: transferência de dados de um banco de dados a outro, mantido ou não pelo mesmo proprietário, com finalidade semelhante ou distinta;

XI - bloqueio: a conservação do dado pessoal ou do banco de dados com a suspensão temporária de qualquer operação de tratamento;

XII - cancelamento: a eliminação ou destruição de dados ou conjunto de dados armazenados em banco de dados, seja qual for o procedimento empregado;

XIII - dissociação: ato de modificar o dado pessoal de modo a que ele não possa ser associado, direta ou indiretamente, com um indivíduo identificado ou identificável;

XIV - dados anônimos: dados relativos a um titular que não possa ser identificado, nem pelo responsável pelo tratamento nem por qualquer outra pessoa, tendo em conta o conjunto de meios suscetíveis de serem razoavelmente utilizados pelo responsável pelo tratamento dos dados ou por qualquer outra pessoa para identificar o referido titular;

Art. 5º O tratamento de dados pessoais por parte de pessoas jurídicas de direito público é permitido para o cumprimento de suas funções institucionais, dentro dos limites da lei.

Art. 6º O tratamento de dados pessoais é atividade de risco e todo aquele que, por meio do tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, é obrigado a ressarci-lo, nos termos da lei.

Art. 7º A defesa dos interesses e direitos dos titulares de dados poderá ser exercida em juízo individualmente ou a título coletivo, na forma do disposto nos artigos 81 e 82 da Lei 8.078, de 11 de setembro de 1990, na Lei 7.347 de 24 de julho de 1985 e nos demais instrumentos de tutela coletiva estabelecidos em Lei.

CAPÍTULO II

PRINCÍPIOS GERAIS DE PROTEÇÃO DE DADOS

Art. 8º Os responsáveis pelo tratamento de dados pessoais deverão atender, dentre outros, aos seguintes princípios gerais de proteção de dados pessoais:

I - Princípio da finalidade: a não utilização dos dados pessoais objeto de tratamento para finalidades distintas ou incompatíveis com aquelas que fundamentaram a sua coleta e que tenham sido informadas ao titular; bem como a limitação deste tratamento às finalidades determinadas, explícitas e legítimas do responsável;

II - Princípio da necessidade: a limitação da utilização de dados pessoais ao mínimo necessário, de forma a excluir o seu tratamento sempre que a finalidade que se procura atingir possa ser igualmente realizada com a utilização de dados anônimos ou com o recurso a meios que permitam a identificação do interessado somente em caso de necessidade;

III - Princípio do livre acesso: a possibilidade de consulta gratuita, pelo titular, de seus dados pessoais, bem como de suas modalidades de tratamento;

IV - Princípio da proporcionalidade: o tratamento de dados pessoais apenas nos casos em que houver relevância e pertinência em relação à finalidade para a qual foram coletados;

V - Princípio da qualidade dos dados: a exatidão dos dados pessoais objeto de tratamento, com atualização realizada segundo a periodicidade necessária para o cumprimento da finalidade de seu tratamento;

VI - Princípio da transparência: a informação ao titular sobre a realização do tratamento de seus dados pessoais, com indicação da sua finalidade, categorias de dados tratados, período de conservação destes e demais informações relevantes;

VII - Princípio da segurança física e lógica: o uso, pelo responsável pelo tratamento de dados, de medidas técnicas e administrativas proporcionais **ao atual estado da tecnologia, à natureza dos dados e às características específicas do tratamento**, constantemente atualizadas e aptas a proteger os dados pessoais sob sua

responsabilidade da destruição, perda, alteração e difusão, acidentais ou ilícitas, ou do acesso não autorizado;

VIII - Princípio da boa-fé objetiva: o respeito à lealdade e à boa-fé objetiva no tratamento de dados pessoais; e

IX - Princípio da responsabilidade: a reparação, nos termos da lei, dos danos causados aos titulares dos dados pessoais, sejam estes patrimoniais ou morais, individuais ou coletivos.

X – Princípio da prevenção: o dever do responsável de, para além das disposições específicas desta Lei, adotar, sempre que possível, medidas capazes de prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

CAPÍTULO III

REQUISITOS PARA O TRATAMENTO DE DADOS PESSOAIS

Art. 9º O tratamento de dados pessoais somente pode ocorrer após o consentimento livre, expresso e informado do titular, que poderá ser dado por escrito ou por outro meio que o certifique, após a notificação prévia ao titular das informações constantes no art. 11.

§ 1º Nos serviços de execução continuada, o consentimento deverá ser renovado periodicamente, nos termos do regulamento.

§ 2º O tratamento de dados pessoais de crianças somente será possível com o consentimento dos responsáveis legais e no seu melhor interesse, sendo vedada a utilização destes dados para finalidades comerciais.

Art. 10. O consentimento pode ser revogado a qualquer momento.

Art. 11. No momento da coleta de dados pessoais, o titular será informado de forma clara e explícita sobre:

I - a finalidade para a qual os seus dados pessoais estão sendo coletados e de que forma serão tratados;

II – a identidade e o domicílio do responsável pelo tratamento;

III - a natureza obrigatória ou facultativa do fornecimento dos dados;

IV - as conseqüências de uma eventual negativa em fornecê-los;

V - os sujeitos para os quais os dados podem ser comunicados e o seu âmbito de difusão; e

VI - os seus direitos, em particular da possibilidade de negar-se a fornecer os dados pessoais e sobre o seu direito de acesso e retificação gratuitos.

Parágrafo único. Considera-se nulo o consentimento prestado caso as referidas informações tenham conteúdo enganoso ou não tenham sido fornecidas de forma clara

e explícita.

Art. 12. O consentimento, caso prestado em conjunto com outras declarações, deve figurar de forma expressa e apartada.

Art. 13. O consentimento será dispensado quando o tratamento:

I - for necessário para a execução de obrigações derivadas de um contrato do qual é parte o titular, para a execução de procedimentos pré-contratuais requeridos por este, ou para o cumprimento de uma obrigação legal por parte do responsável;

II - referir-se a dados provenientes de registros, atos ou documentos públicos de acesso público irrestrito;

III - for necessário para o exercício de funções próprias dos poderes do Estado;

IV - for realizado unicamente com finalidades de pesquisa histórica, científica ou estatística;

V - for necessário para a proteção da vida ou da incolumidade física do titular ou de um terceiro, nos casos em que o titular não possa prestar o próprio consentimento por impossibilidade física ou por incapacidade de compreensão;

VI - for necessário para o exercício do direito de defesa ou para fazer valer um direito em sede judicial, desde que os dados coletados sejam tratados exclusivamente para esta finalidade e estritamente pelo período de tempo necessário para sua execução;

VII - disser respeito a dados sobre o inadimplemento de obrigações por parte do titular, caso em que o titular deverá ser notificado previamente por escrito, nos termos do art. 43 da Lei 8.078/90 – Código de Defesa do Consumidor.

Art. 14. Os dados pessoais que forem objeto de tratamento deverão ser:

I - tratados de forma lícita e com boa-fé;

II - coletados e armazenados para finalidades determinadas, explícitas e legítimas;

III – exatos, claros, objetivos, atualizados e de fácil compreensão;

IV - pertinentes, completos, proporcionais e não excessivos em relação à finalidade que justificou sua coleta ou tratamento posterior;

V - conservados de forma a permitir a identificação de seu titular por um período de tempo não superior ao necessário para as finalidades que justificaram sua coleta ou tratamento posterior; e

VI - conservados por período não superior ao estabelecido em lei ou regulamento específico para cada setor.

§ 1º É vedado o tratamento de dados pessoais obtidos por meio de erro, dolo, coação e lesão.

§ 2º Os dados pessoais obtidos ou tratados de forma contrária à presente lei e à disciplina referente à proteção de dados não poderão ser utilizados e deverão ser cancelados.

CAPÍTULO IV

DOS DIREITOS DO TITULAR

Art. 15. O titular dos dados poderá obter do responsável pelo tratamento a confirmação da existência de dados pessoais que lhe digam respeito, bem como o acesso aos dados em si, tanto diretamente, como por meio da ação de *habeas data, nos termos da lei*.

§ 1º As informações requeridas serão fornecidas, imediatamente, de forma simplificada ou, no prazo de 5 (cinco) dias, por meio de um extrato claro e completo, abrangendo a informação sobre a sua origem, bem como sobre a lógica, os critérios utilizados e a finalidade do respectivo tratamento.

§ 2º O fornecimento destas informações não importa em ônus para o titular dos dados.

§ 3º Estas informações, por escolha do titular, poderão ser fornecidas por escrito ou por meio eletrônico, seguro e idôneo para tal fim.

§ 4º A informação deve ser ampla e versar sobre a totalidade do registro existente, mesmo quando o requerimento compreender somente um aspecto dos dados pessoais do titular.

§ 5º Os dados pessoais serão armazenados de forma que permitam o exercício do direito de acesso.

Art. 16. Mediante solicitação do titular dos dados, o responsável deverá, sem ônus, no prazo de 5 (cinco) dias:

I - corrigir os dados pessoais que forem incompletos, inexatos ou desatualizados;

II - cancelar, dissociar ou bloquear os dados pessoais que forem desnecessários, excessivos ou tratados em desconformidade com a presente lei.

Parágrafo único. O responsável obriga-se, no prazo de 5 (cinco) dias, a comunicar aos destinatários das informações a realização de correção, cancelamento, dissociação e bloqueio dos dados.

Art. 17. O titular dos dados poderá opor-se, total ou parcialmente, ao tratamento de seus dados pessoais:

I - sempre que tiver motivos legítimos, salvo nos casos em que o tratamento seja necessário para o cumprimento de uma obrigação imposta pela lei à pessoa responsável;

II - quando seus dados forem utilizados para fins publicitários, ainda que tenham sido submetidos a um procedimento de dissociação.

Art. 18. Nos casos de descumprimento desta lei, o titular poderá pleitear os seus direitos perante a Autoridade de Garantia, na forma do regulamento.

Art. 19. O titular dos dados tem direito a não ser submetido a decisões que lhe afetem, de maneira significativa, unicamente com base em um tratamento automatizado de dados pessoais destinado a definir o perfil ou a personalidade do titular.

§ 1º Qualquer decisão desta natureza pode ser impugnada pelo titular, que tem o direito de obter informações do responsável pelo tratamento a respeito dos critérios desta avaliação e sobre o procedimento em que esta se baseou.

§ 2º Admite-se esta modalidade de decisão nos casos em que tenha sido expressamente solicitada pelo titular e desde que garantidos o devido processo legal e a ampla defesa.

CAPÍTULO V

TRATAMENTO DE DADOS SENSÍVEIS

Art. 20. Nenhuma pessoa pode ser obrigada a fornecer dados sensíveis.

Art. 21. É proibida a formação de bancos de dados que contenham informações que, direta ou indiretamente, revelem dados sensíveis, salvo disposição legal expressa, respeitados os direitos de personalidade do titular, em especial a garantia de não discriminação.

§ 1º O tratamento de dados sensíveis será permitido quando:

I - o titular tiver dado o seu consentimento livre, informado e por escrito, sempre que este tratamento for indispensável para o legítimo exercício das atribuições legais ou estatutárias de seus responsáveis.

II - for realizado por associações e outras entidades sem fins lucrativos de natureza política, filosófica, religiosa ou sindical para a realização de finalidades lícitas e compreendendo os dados pessoais de seus inscritos, sempre que os dados não sejam comunicados ou difundidos para terceiros e quando o ente em questão determine medidas idôneas de garantia dos direitos do titular para o tratamento realizado;

III - for necessário para a proteção da vida ou da incolumidade física do titular ou de um terceiro, nos casos em que o titular não possa prestar o próprio consentimento por impossibilidade física ou por incapacidade de compreensão; ou

IV - for realizado unicamente com finalidades de pesquisa histórica, científica ou estatística;

V - for relativo a dados manifestamente tornados públicos pelo seu titular.

VI - for realizado por profissionais da área da saúde ou entidades sanitárias e se mostrar indispensável para a tutela da saúde do interessado.

VII – for necessário para o exercício de funções próprias dos poderes de Estado, previstas em lei.

§ 2º Em qualquer hipótese, considerar-se-á ilegal o tratamento de dados sensíveis que for utilizado para fins discriminatórios.

Art. 22. A Autoridade de Garantia poderá indicar medidas de segurança e de proteção ao titular de dados sensíveis que deverão ser adotadas pelo responsável pelo tratamento.

CAPÍTULO VI

SEGURANÇA DOS DADOS

Art. 23. O tratamento de dados pessoais será feito de modo a reduzir ao mínimo, mediante a adoção de medidas idôneas de segurança preventiva, o risco de sua destruição ou perda, de acesso não autorizado ou de tratamento não permitido pelo titular ou diverso da finalidade da sua coleta, independentemente do motivo.

Parágrafo único. As medidas referidas no caput devem ser proporcionais ao atual estado da tecnologia, à natureza dos dados e às características específicas do tratamento, em particular no caso do tratamento de dados sensíveis.

Art. 24. Um conjunto de medidas mínimas de segurança preventiva será publicado pela Autoridade de Garantia dentro de, no máximo, um ano após a entrada em vigor da presente lei, e atualizado periodicamente, com base na evolução da tecnologia e na experiência adquirida.

Art. 25. O subcontratado deve ter experiência, capacidade e idoneidade para garantir o respeito às disposições vigentes em matéria de tratamento de dados pessoais, e responderá solidariamente com o responsável pelos prejuízos causados pela sua atividade aos titulares dos dados.

Parágrafo único. O subcontratado deverá realizar o tratamento segundo as instruções fornecidas por escrito pelo responsável, que, mediante inspeções periódicas, verificará a observância das próprias instruções e das normas sobre a matéria.

Art. 26 O responsável, o subcontratado ou qualquer outra pessoa que intervenha em qualquer fase do tratamento de dados pessoais obriga-se ao dever de segredo em relação aos mesmos, dever este que permanece após o término do respectivo tratamento ou do vínculo empregatício existente.

Art. 27. O responsável pelo tratamento deverá comunicar à Autoridade de Garantia e aos titulares dos dados, imediatamente, sobre o acesso indevido, perda ou difusão acidental, seja total ou parcial, de dados pessoais, sempre que este acesso, perda ou difusão acarretem riscos à privacidade dos seus titulares.

Parágrafo único. Nos casos mencionados no caput, a Autoridade de Garantia poderá tomar as providências que julgar necessárias, no âmbito de suas competências, inclusive determinando ao responsável a ampla divulgação do fato em meios de comunicação.

CAPÍTULO VII

COMUNICAÇÃO E INTERCONEXÃO DOS DADOS PESSOAIS

Art. 28. A comunicação ou a interconexão dos dados pessoais somente será permitida com o consentimento livre e expresso do titular e para o cumprimento de fins diretamente relacionados com as funções legítimas do cedente e do cessionário.

§ 1º O consentimento para a comunicação ou interconexão é revogável a qualquer tempo.

§ 2º O consentimento será dispensado quando:

I - os dados forem provenientes de registros, atos ou documentos públicos acessíveis a qualquer pessoa, levando em consideração os limites estabelecidos para o acesso e publicidade destes dados;

II - para o cumprimento de uma obrigação prevista em lei;

III - quando for necessária para a proteção da vida ou da incolumidade física do titular ou de um terceiro, nos casos em que o titular não possa prestar o próprio consentimento por impossibilidade física ou por incapacidade de compreensão.

Art. 29. O cessionário ficará sujeito às mesmas obrigações legais e regulamentares do cedente, inclusive quanto à responsabilidade solidária pelos danos eventualmente causados e ao dever de receber e processar impugnação e realizar correções.

CAPÍTULO VIII

DO TÉRMINO DO TRATAMENTO DOS DADOS PESSOAIS

Art. 30. Os dados pessoais serão cancelados quando deixarem de ser necessários ou pertinentes para a finalidade que justificou sua coleta e tratamento.

Parágrafo único. Lei ou regulamento poderá dispor sobre períodos máximos para o tratamento de dados pessoais em setores e situações específicas.

Art. 31. No término do tratamento dos dados pessoais, sem prejuízo dos direitos do titular, e sempre que houver necessidade ou pertinência, os dados podem ser:

I - cedidos a terceiros, desde que destinados a tratamento para finalidades análogas àquelas para as quais foram colhidas e mediante o consentimento dos titulares;

II - conservados para fins exclusivamente pessoais e não destinados à comunicação ou

à difusão;

III - conservados ou cedidos a terceiro, unicamente para finalidades históricas, estatísticas ou de pesquisa científica.

CAPÍTULO IX

TRATAMENTO DE DADOS PESSOAIS NO SETOR PÚBLICO

Art. 32. A comunicação e interconexão de dados pessoais entre pessoas jurídicas de direito público será admitida nos casos em que suas competências não versem sobre matérias distintas, respeitados os direitos estabelecidos nesta lei.

Parágrafo único. A comunicação de dados pessoais entre pessoas jurídicas de direito público com competências sobre matérias distintas será admitida:

I - mediante expressa previsão legal, sempre no respeito aos direitos dos titulares dos dados; ou

II - quando for necessária para a realização das suas competências institucionais.

Art. 33. Os responsáveis pelos bancos de dados públicos poderão, mediante decisão fundamentada e somente pelo período necessário, negar o cancelamento e a oposição ao tratamento dos dados pessoais, quando for indispensável para:

I - a proteção da ordem pública;

II - a proteção de direitos de terceiros;

III – não obstaculizar a atuação judicial ou administrativa em curso, vinculadas à investigação sobre o cumprimento de obrigações tributárias, o desenvolvimento de funções de controle da saúde e do meio ambiente e a verificação de infrações administrativas.

CAPÍTULO X

TRATAMENTO DE DADOS PESSOAIS NO SETOR PRIVADO

Art. 34. Toda entidade privada que realize o tratamento de dados pessoais para o desenvolvimento de suas atividades e conte com mais de duzentos empregados deverá apontar um diretor responsável pelo tratamento de dados pessoais.

§ 1º O diretor responsável pelo tratamento de dados pessoais deverá zelar, de forma independente, pela observância das disposições da presente lei.

§ 2º As atividades do diretor responsável pelo tratamento de dados pessoais

consistem, entre outras, em:

I – atuar como o correspondente imediato da Autoridade de Garantia;

II - orientar os demais funcionários a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

III - manter uma relação dos tratamentos de dados pessoais realizados pela empresa, imediatamente acessível pelos titulares que requisitem seus próprios dados pessoais.

§ 3º A entidade informará à Autoridade de Garantia sobre a identidade do diretor responsável pelo tratamento de dados pessoais.

CAPÍTULO XI

TRANSFERÊNCIA INTERNACIONAL DE DADOS

Art. 35. A transferência internacional de dados pessoais somente é permitida para países que proporcionem um nível de proteção de dados equiparável ao da presente lei, salvo as seguintes exceções:

I - quando o titular tiver manifestado o próprio consentimento livre, expresso e informado para a transferência;

II - quando for necessária para a execução de obrigações derivadas de um contrato do qual o titular for parte;

III - quando for necessária para a garantia de um interesse público relevante previsto em lei;

IV – quando for necessária para a cooperação internacional entre órgãos públicos de inteligência e de investigação, de acordo com os instrumentos de direito internacional a que o Brasil se vincule;

V - quando for necessária para a defesa de um direito em juízo, se os dados forem transferidos exclusivamente para esta finalidade e pelo período de tempo necessário;

VI - quando for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro, se o titular não puder fornecer o próprio consentimento por impossibilidade física, por incapacidade de agir ou de compreender.

Art. 36. A Autoridade de Garantia reconhecerá o caráter adequado do nível de proteção de dados do país de destino levando em conta a legislação em vigor neste país e as demais circunstâncias relativas à transferência de dados.

Parágrafo único. Para os fins do previsto no caput, a Autoridade considerará a natureza dos dados, as normas gerais e setoriais presentes em seu ordenamento, a observância dos princípios de proteção de dados e das medidas de segurança previstas.

Art. 37. A Autoridade de Garantia poderá autorizar uma transferência ou série de transferências para um país estrangeiro que não disponha de um nível adequado de proteção quando o responsável pelo tratamento ofereça garantias suficientes em relação à proteção da privacidade dos titulares, às medidas de segurança adotadas e a possibilidade do exercício dos direitos dispostos nesta lei.

Parágrafo único. A transferência de dados pessoais ao exterior, neste caso, somente poderá ocorrer após a autorização expressa da Autoridade de Garantia.

TÍTULO II

TUTELA ADMINISTRATIVA

CAPÍTULO I

AUTORIDADE DE GARANTIA

Art. 38. É criado o Conselho Nacional de Proteção de Dados Pessoais, com autonomia administrativa, orçamentária e financeira, com a atribuição de atuar como Autoridade de Garantia quanto à proteção de dados pessoais, cuja estrutura e atribuições serão estabelecidas em legislação específica.

Art. 39. Compete ao Conselho Nacional de Proteção de Dados Pessoais:

I - zelar pela observância desta lei, de seu regulamento e do seu regimento interno;

II - planejar, elaborar, propor, coordenar e executar ações da política nacional de proteção de dados pessoais;

III - editar normas e provimentos sobre matérias de sua competência;

IV - aprovar seu regimento interno;

V - receber, analisar, avaliar e encaminhar consultas, denúncias, reclamações ou sugestões apresentadas por titulares de dados pessoais, entidades representativas ou pessoas jurídicas de direito público ou privado, referentes à proteção de dados pessoais, nos termos do regulamento;

VI – aplicar, de ofício ou a pedido de parte, conforme o caso, sanções, medidas corretivas e medidas preventivas que considere necessárias, na forma desta lei;

VII – criar, manter e publicar, para fins de transparência, um registro de bancos de

dados pessoais de caráter de categorias e setores que considere relevantes, nos termos de regulamento;

VIII - verificar se os tratamentos respeitam as normas legais e os princípios gerais de proteção de dados;

IX - promover o conhecimento entre a população das normas que tratam da matéria e de suas finalidades, bem como das medidas de segurança de dados;

X - vetar, total ou parcialmente, o tratamento de dados ou prover seu bloqueio se o tratamento se torna ilícito ou inadequado, nos termos de regulamento;

XI - reconhecer o caráter adequado do nível de proteção de dados do país de destino no caso de transferência internacional de dados pessoais, bem como autorizar uma transferência ou série de transferências para países terceiros que não contem com este nível adequado;
XII – determinar ao responsável pelo tratamento de dados pessoais, quando necessário, a realização de estudo de impacto à privacidade, na forma de regulamento.

XIII - desenvolver outras atividades compatíveis com suas finalidades.

Art. 40. Os Estados, o Distrito Federal e os Municípios poderão criar suas próprias autoridades de proteção de dados pessoais, com competência concorrente e nas suas respectivas áreas de atuação administrativa.

CAPÍTULO II

SANÇÕES ADMINISTRATIVAS

Art. 41. Sem prejuízo das sanções civis e penais cabíveis e de outras sanções administrativas a serem definidas em normas específicas, as infrações das normas previstas nesta Lei ficam sujeitas, conforme o caso, às seguintes sanções administrativas:

I - multa;

II – bloqueio dos dados pessoais;

III – dissociação dos dados pessoais;

IV – cancelamento dos dados pessoais;

V – proibição do tratamento de dados sensíveis;

VI – suspensão temporária de atividade; e

VII – proibição de funcionamento do banco de dados.

§ 1º As sanções previstas neste artigo serão aplicadas pela Autoridade de Garantia, no âmbito de sua atribuição, podendo ser aplicadas cumulativamente, inclusive por medida cautelar, antecedente ou incidente de procedimento administrativo.

§ 2º As condições e procedimentos para a aplicação das sanções previstas, que devem ser graduadas em razão da gravidade, extensão da violação, natureza dos direitos pessoais afetados, reincidência e dos prejuízos dela derivados, serão determinados por meio de regulamentação.

Art. 42. A multa será estipulada:

I - no caso de empresa, em até vinte por cento do valor do faturamento bruto no seu último exercício, excluídos os impostos;

II - No caso das demais pessoas físicas ou jurídicas de direito público ou privado, bem como quaisquer associações de entidades ou pessoas constituídas de fato ou de direito, ainda que temporariamente, com ou sem personalidade jurídica, não sendo possível utilizar-se o critério do valor do faturamento bruto, em montante não inferior a R$ 2.000,00 (dois mil reais) e não superior a R$ 6.000.000,00 (seis milhões de reais).

Parágrafo único. Em caso de reincidência, as multas cominadas serão aplicadas em dobro, não se aplicando, em tal hipótese, o limite máximo indicado no inciso II.

Art. 43. Sem prejuízo das sanções cabíveis, a Autoridade de Garantia, atuando de ofício ou a pedido de parte, deverá impor, aos responsáveis que incorram em infração às normas desta lei, as medidas corretivas que considere necessárias para reverter os efeitos danosos que a conduta infratora tenha causado ou para evitar que esta se produza novamente no futuro, fixando o valor da multa diária pelo seu descumprimento.

§ 1º As decisões administrativas transitadas em julgado que apliquem medidas corretivas em favor do titular dos dados constituem título executivo extrajudicial.

§ 2º Sempre que as medidas corretivas se dirigirem a um titular específico, é deste a legitimidade para executar a decisão.

Art. 44. Em qualquer fase do processo administrativo é facultado à Autoridade de Garantia adotar medidas preventivas, de ofício ou a pedido de parte, quando houver indício ou fundado receio de que o representado, direta ou indiretamente, cause ou possa causar à coletividade lesão irreparável ou de difícil reparação no âmbito da proteção de dados pessoais, ou torne ineficaz o resultado final do processo, fixando o valor da multa diária pelo seu descumprimento.

TÍTULO III

CÓDIGOS DE BOAS PRÁTICAS

Art. 45. Os responsáveis pelo tratamento de dados pessoais, individualmente ou através de organizações de classe, poderão formular códigos de boas práticas que estabeleçam as condições de organização, regime de funcionamento, procedimentos aplicáveis, normas de segurança, padrões técnicos, obrigações específicas para os diversos envolvidos no tratamento e no uso de dados pessoais e demais quesitos e garantias para as pessoas, com pleno respeito aos princípios e disposições da presente lei e demais normas referentes à proteção de dados.

§ 1º Os códigos de boas práticas vincularão os respectivos responsáveis pelo tratamento de dados e os membros de uma determinada classe profissional.

§ 2º A Autoridade de Garantia solicitará às respectivas organizações de classe a elaboração dos códigos de boas práticas quando julgar conveniente e poderá participar de sua elaboração.

§ 3º Entre outras categorias profissionais, a Autoridade de Garantia priorizará o fomento à elaboração de códigos de boas práticas em tema de:

I - vigilância e monitoramento;

II - publicidade e marketing direto;

III - bancos de dados de proteção ao crédito;

IV - seguros; e

V - demais matérias pertinentes.

§ 4º Os códigos de boas práticas serão depositados na Autoridade de Garantia, que poderá não aprová-los se estiverem em desconformidade com as disposições legais e regulamentares sobre a matéria, ao que seguirá uma solicitação para que sejam feitas as modificações necessárias e indicadas.

§ 5º Os códigos de boas práticas serão disponibilizados publicamente e deverão ser atualizados sempre que se demonstrar necessário.

TÍTULO IV

DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 46. Os direitos previstos nesta lei não excluem outros, decorrentes de tratados ou convenções internacionais de que o Brasil seja signatário, da legislação interna

ordinária, bem como de regulamentos expedidos pelas autoridades administrativas competentes.

Art. 47. Ficam revogados os artigos de 2º, 3° e 4º da Lei 9.507, de 12 de novembro de 1997.

Art. 48. Esta Lei entrará em vigor no prazo de 90 dias contados da data da sua publicação.